

Susan M. Rotkis, AZ Bar 032866
Consumer Litigation Associates West, PLLC
382 S. Convent Ave.
Tucson, AZ 85716
520-622-2481
srotkis@clalegal.com

Leonard A. Bennett
admission pro hac vice requested
Consumer Litigation Associates, P.C.
763 J. Clyde Morris Blvd, Suite 1-A
Newport News, VA 23601
757-930-3660
lenbennett@clalegal.com

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

**CORINNE COOPER, MORGAN
RUTHERFORD, DONNA DECONCINI,**
*on behalf of themselves and all others
similarly situated,*

Plaintiffs,

v.

**EQUIFAX. INC., a Georgia
corporation,
SERVE: registered agent**
Prentice-Hall Corp System
2338 W. Royal Palm Rd
Phoenix, AZ 85021

**EQUIFAX INFORMATION SERVICES,
LLC, a foreign limited liability company, and
SERVE: registered agent**
Corporation Service Company
2338 W Royal Palm Rd Ste-J
Phoenix, AZ 85021

Case No.:

CLASS ACTION COMPLAINT

**EQUIFAX CONSUMER SERVICES LLC, a
Georgia limited liability company,
Defendants.**

COME NOW Plaintiffs, Corinne Cooper, Morgan Rutherford, and Donna DeConcini, on behalf of themselves and all other consumers similarly situated, by counsel, seek judgment against Defendants Equifax, Inc., Equifax Information Services, LLC (“EIS”), and Equifax Consumer Services LLC (“ECS”) (collectively, “Equifax”), and state as follows:

I. PRELIMINARY STATEMENT

1. This is an action for damages, costs, and attorneys’ fees brought pursuant to common-law negligence. Defendants negligently allowed the fraudulent procurement of the critical private information of class member consumer report files, and failed to disclose the fact of such procurement from plaintiffs.

2. Defendants operate together as a unified consumer reporting agency (“CRA”) to prepare and furnish consumer reports for credit and other purposes. Equifax’s databases contain a treasure trove of valuable information about nearly every American adult—account numbers and payment histories, Social Security numbers, names and aliases, birthdates, addresses, employment histories, and the like—that Equifax collects and sells to businesses that extend credit, loan money, sell insurance, and grant employment, among numerous other activities.

3. Defendants obtain the largest portion of their vast store of data independently and without consumers’ consent or knowledge. Put differently, consumers rarely turn data over to

1 Equifax knowingly and willingly—most of the data Equifax possesses it obtained from sources
2 other than the consumers themselves.
3

4 4. By now, the Court well familiar with the “Equifax breach” and, possibly,
5 Defendant’s response to it including testimony in front of several congressional committees on
6 October 3, 2017.

7 5. In May of 2017, and likely earlier, unknown individuals electronically accessed
8 Equifax’s databases without Defendants’ knowledge, gaining access to information about
9 approximately 145,500,000 Americans.¹ Ironically, the identity thieves entered Equifax’s systems
10 through the Internet portal it uses to receive consumer disputes of identity theft and other credit
11 inaccuracies,² and then accessed collateral database information from there, including Defendant’s
12 core consumer contact database, “ACIS.”³
13
14

15 6. Defendants have disclosed generally that the fraudulent users procured consumers’
16 names, Social Security numbers, birthdates, addresses, and driver’s license numbers.⁴ Thus,
17 Equifax furnished this information to the fraudulent users. The breach lasted for months and,
18 although Equifax knew about the security vulnerability in May, and the breach itself in July at the
19 latest, it sat on this information until September 8, 2017.
20

21
22
23 ¹ See <https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do>

24 ² Equifax had created that portal as a means to fully automate its “reinvestigations” of consumer
25 disputes and – in theory – avoid the expense of having live human beings oversee that process
and obligation.

26 ³ “ACIS” is Equifax’s acronym for its “Automated Consumer Interview System”.

27 ⁴ <https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832>.

8. Plaintiffs include Arizona and National consumers regarding whom Defendants possessed information protected by the federal Fair Credit Reporting Act, which was thereafter unlawfully procured by identity thieves between March and July 2017.

1 10. The Court has diversity jurisdiction as to all Plaintiffs and all class members
2 pursuant to 28 U.S.C. § 1332(a) as all Plaintiffs seek to recover damages in excess of \$75,000
3 individually for actual damages and every Plaintiff is diverse from Defendants.
4

5 11. The Court also has diversity jurisdiction pursuant to 28 U.S.C. §1332(d), as none
6 of the Plaintiffs are from the same state as Defendants, more than two-thirds of each putative class
7 resides and is legally domiciled in a state other than Georgia or that of Defendants, there are at
8 least tens of thousands of class members and the total amount that will be recovered in damages
9 will exceed \$5 million.
10

11 12. Defendant Equifax is a corporation headquartered in Atlanta, Georgia, and
12 Plaintiffs and all consumers embraced by the Class definition below reside in the District of
13 Arizona.
14

15 13. Defendant Equifax is subject to personal jurisdiction in the District of Arizona, by
16 virtue of the business it conducts in the Division. Further, it deliberately and specifically availed
17 itself of the benefits of Arizona and caused direct injury to Arizona consumers, including the
18 Plaintiffs, in Arizona.
19

20 14. The Court also has subject matter jurisdiction as each Plaintiff suffered real and
21 definite harm. Defendants confirmed that the core personal information maintained by Equifax
22 was furnished to and procured by criminal data thieves. They will now spend the rest of their lives
23 worried about, fearful of and having to expend time and money to prevent credit, criminal, tax
24 filing and other identity theft events. Further, Plaintiffs also suffered tangible injury in the value
25 of the credit monitoring service they were denied.
26

III. PARTIES

15. Each representative Plaintiff is a natural person. The putative class is comprised of natural persons, all of whom are consumers as defined by the Fair Credit Reporting Act (“FCRA”) 15 U.S.C. § 1681 et seq.

16. Each Plaintiff named herein has reason to believe, based upon the public reports of the Data Breach, its scale, and upon information provided by Equifax via its website, that his or her personal identifying information (“PII”) was taken during the Data Breach.

17. Plaintiff Corinne Cooper is a resident of Tucson, Arizona. In or about September of 2017, Ms. Cooper visited the Equifax website which stated to her that she may be a victim of the Data Breach. Ms. Cooper has devoted significant time to monitoring her accounts in response to the Data Breach, including by activating credit “freezes” at Equifax, TransUnion LLC, and Experian Information Solutions, LLC, and Innovis. She has had to pay money to at least one additional consumer reporting agency to have her credit freeze initiated. She was never alerted or advised by Equifax that her consumer report information had been procured as a result of the Data Breach.

18. Plaintiff Morgan Rutherford is a resident of Tucson, Arizona. In or about September of 2017, Ms. Rutherford visited the Equifax website which stated to her that she may be a victim of the Data Breach. Ms. Rutherford has devoted significant time to monitoring her accounts in response to the Data Breach, including initiating credit freezes. She was never alerted

1 or advised by Equifax that her consumer report information had been procured as a result of the
2 Data Breach.
3

4 19. Plaintiff Donna DeConcini is a resident of Tucson, Arizona. In or about September
5 of 2017, Ms. DeConcini visited the Equifax website which stated to her that she may be a victim
6 of the Data Breach. Ms. DeConcini has devoted significant time to monitoring her accounts in
7 response to the Data Breach, including initiating credit freezes. She was never alerted or advised
8 by Equifax that her consumer report information had been procured as a result of the Data Breach.
9

10 20. All three Defendants are both “consumer reporting agencies” and “nationwide
11 consumer reporting agencies” as defined and governed un the FCRA.
12

13 21. Defendant Equifax, Inc. is the parent of the two additional Defendants. In prior
14 litigation, it has taken the position that it is not itself a “consumer reporting agency” governed by
15 the FCRA. *See* 15 U.S.C. § 1681a(f) (“The term “consumer reporting agency” means any person
16 which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or
17 in part in the practice of assembling or evaluating consumer credit information or other information
18 on consumers for the purpose of furnishing consumer reports to third parties, and which uses any
19 means or facility of interstate commerce for the purpose of preparing or furnishing consumer
20 reports.”)
21

22 22. But of course, Equifax, Inc. *is* a consumer reporting agency. For purposes of the
23 FCRA, Equifax, Inc. has held itself out repeatedly to consumers, regulators and the public
24 generally as the actual operating entity. The branding, labels and disclosures on the Defendants’
25
26
27
28

1 consumer website is dominated by “Equifax, Inc.” titling. Defendants have held Equifax, Inc. out
2 as the operating and responsible entity.
3

4 23. Defendant Equifax Consumer Services, LLC is similarly a CRA. It for monetary
5 fees, regularly engages in part in the practice of assembling and maintaining consumer report
6 information in its operational relationship with Equifax, Inc. and EIS.
7

8 24. Defendant Equifax Information Services, LLC is a foreign limited liability
9 company transacting business in Arizona and maintains a registered agent office in Phoenix. At
10 all times relevant to this action, EIS has acknowledged that it is and was a “consumer reporting
11 agency” as defined by the Fair Credit Reporting Act, § 1681a(f).
12

13 25. The FCRA, through a rule mandated at § 1681x, expressly prohibits “a consumer
14 reporting agency from circumventing or evading treatment as a consumer reporting agency” by
15 means of corporate reorganization or structuring.

16 26. Equifax, Inc. and its subsidiaries – whether or not they observe state law corporate
17 formalities – have eliminated nearly all lines between their different business entities in the
18 collection, maintenance, sharing and furnishing of consumer reporting information. Equifax, Inc.,
19 entities such as EIS regularly share FCRA restricted information with sibling entity ECS to market
20 and profit from the sale of consumer identity theft prevention products, including the blurring of
21 legal lines between providing file information under the FCRA versus for private sale to the
22 consumer. Equifax subsidiary TALX Corporation operates as Equifax Workforce Solutions, and
23 with control of acquired-entity eThority and both provides and obtains FCRA-governed consumer
24 information to and from other Equifax entities. Equifax entity Anakam, Inc. integrates Equifax
25
26
27
28

1 consumer data for sale of its fraud detection and verification products, largely now under the
2 Equifax brand. And, by last example Equifax Mortgage Services operates as a separate entity
3 focused on the mortgage services industry, but also freely shares and uses otherwise FCRA
4 protected data.
5

6 27. Further, throughout this breach and post-exposure conduct, the Defendants have
7 operated and acted as one entity and CRA.
8

9 28. Here, Equifax, Inc. has used EIS and ECS as dependent and integrated divisions
10 rather than as separate legal entities. The business operations are fully coordinated and shared.
11 Resources are cross-applied without full and complete cost and profit centers. Management
12 decisions at EIS and ECS are made by and through management at Equifax, Inc. And the entities
13 largely hold themselves out as a single uniform business.
14

15 29. For purposes of the claims here, these facts are especially meaningful. Data
16 security was shared and the negligence here was directly that of management officials at Equifax,
17 Inc. In fact, it was Equifax, Inc.'s Chief Security Officer Susan Mauldin and Chief Information
18 Officer David Webb who Defendants have fired as a result of the events alleged herein, rather than
19 employees of the subsidiary entities. Equifax, Inc.'s president has directed all matters related to
20 these events. And Equifax, Inc.'s General Counsel was and has remained the Chief Legal Officer
21 and compliance official for all Equifax entities as of October 3, 2017. Equifax's Chief Executive
22 Officer Richard Smith recently resigned, but reportedly was paid \$90 million upon his departure.
23

24 30. To remain separate and distinct for the purposes of liability in this action,
25 Defendants must operate as separate and legally as well as operationally distinct entities. Here,
26

1 for matters and functions alleged and relevant herein, EIS and ECS were merely alter egos of
2 Equifax, Inc. For purposes of how consumer data was handled, warehoused, used and sold, the
3 corporate lines were disregarded in practice. EIS and ECS were mere instrumentalities for the
4 transaction of the corporate consumer credit business. The Defendants shared full unity of interest
5 and ownership such that the separate personalities of the corporation and subsidiaries no longer
6 existed.
7

8
9 31. Further, recognition of the technical corporate formalities in this case would cause
10 an irremediable injustice and permit Equifax, Inc. – the entity whose management ran, caused and
11 permitted the events alleged herein – to defeat justice and to evade tort responsibility. *Heyde v.*
12 *Xtraman, Inc.*, 199 Ga. App. 303, 306, 404 S.E.2d 607 (1991).
13

14 32. Accordingly, for all purposes hereafter, when the Plaintiffs allege “Equifax” as the
15 actor or responsible party, they are alleging the participation and responsibility of all three
16 Defendants collectively.

17 IV. FACTS

18 Equifax Breached its Duty of Care in Causing and Permitting the Data 19 Breach 20

21 33. Equifax’s business is information. It gathers, through third-party submissions and
22 by accessing public and other records, information on nearly every American adult. It sells this
23 information to countless businesses so that they may make decisions such as whether to grant
24 credit, offer employment, loan money, issue insurance, rent housing, and the like. Although
25
26
27

1 Equifax is strictly governed by the FCRA, it also has common-law obligations to secure the
2 information it possesses and protect it from unauthorized dissemination.
3

4 34. Equifax is aware that it is held to a heightened duty of care to protect its consumer
5 file information. The text of its governing statute, the FCRA, itself warns Equifax of its “grave
6 responsibilities” to maintain the privacy of consumer data, language that has been often repeated
7 in court decisions in which Equifax was involved. And the Defendants even acknowledge in their
8 2016 Annual Report that, “We are subject to a number of U.S. and state and foreign laws and
9 regulations relating to consumer privacy, data and financial protection. These regulations are
10 complex, change frequently, have tended to become more stringent over time[.]”
11

12 35. The standard duty of care for Equifax was significant. It possessed – for profit and
13 resale – the very private personal identifiers and financial information on nearly every consumer
14 in the nation. In fact, Equifax possesses significantly greater amounts of that information than
15 even the Federal and State governments, which themselves have to purchase reporting products
16 from Equifax to discover such information. The standard for Equifax’s maintenance and
17 monitoring of its systems is much greater than an ordinary business.
18

19 36. The Gramm–Leach–Bliley Act (“GLBA”), 15 U.S. Code § 6801, and the
20 regulations promulgated thereunder also imposed a duty on Equifax to insure the security and
21 confidentiality of customer records and information, to protect against hazards including
22 unauthorized access or use, and to notify affected customers as soon as possible of any breach of
23 security.
24
25
26
27
28

1 37. Equifax owed these duties, in particular, to Plaintiffs and Class Members, as
2 persons whose personal identifying information (“PII”) and other information was in Equifax’s
3 possession.
4

5 38. Equifax had a special relationship with the Plaintiffs and Class Members because
6 it was entrusted with their personal information. Equifax’s ability to acquire Class Members’ PII
7 and other information from them and other entities, created an independent duty of care because it
8 was predicated on the understanding, based on Equifax’s own representations, that Equifax would
9 take adequate security precautions.
10

11 39. Further, Equifax’s trade in the private and critical financial information of
12 consumers poses an abnormally dangerous risk of financial harm to those consumers.
13

14 40. EIS is the entity that Equifax uses to warehouse and administer the retail credit
15 information and credit reporting function for U.S. consumers. It gathers the information from third
16 parties it labels “subscribers,” referred to as “furnishers” under the FCRA, builds files matching
17 that data to specific consumers and stores it in a database it titles “ACRO.”

18 41. Separately, Equifax maintains the ACIS database which includes all documents
19 created or obtained by Equifax from consumer contacts, such as consumer disputes, requests for a
20 copy of the consumer’s own credit file, correspondence sent to the consumer, and substantial
21 amounts of data generated to document and archive each of these contacts. Communications that
22 come in from the Equifax Internet portal that was the conduit for the data breach are maintained
23 in the ACIS system. And Equifax has tried to convince the public generally that its “core database”
24 was not breached. But that distinction is meaningless as entry into the ACIS system provides
25
26
27
28

1 access to nearly all of the same data – personal identifiers, accounts, etc. – that would be useful
2 from the ACRO database. And access through ACIS gets a user directly into other data troves
3 containing comparable information.
4

5 42. In the modest amount of information that it has released publicly, Equifax admits
6 that its security team first observed suspicious network traffic associated with its U.S. online
7 dispute portal web application no earlier than July 29, 2017 and continuing overnight into July 30,
8 2017.
9

10 43. Equifax cannot state with any certainty when this intrusion began.

11 44. Equifax has represented that the Data Breach occurred when hackers entered its
12 dispute portal through a vulnerability via something called “Apache Struts.”
13

14 45. Apache Struts is an open-source application framework that allows applications to
15 run on a web server.

16 46. At a high level, an application framework can be thought of as “prepackaged”
17 computer code that is specifically designed to allows users to then write their own custom code,
18 add it to the environment, and then allow the prepackaged code portions to run the custom code
19 portions so that in house programmers do not need to reinvent the wheel every time they build an
20 application.
21

22 47. Since application frameworks are specifically designed to incorporate other pieces
23 of code that are not part of the package (in this case, Apache Struts), they are particularly
24 vulnerable to attack since the software is designed to and given permission to run code portions
25 that are custom designed by in house programming teams (or in this case, outsiders).
26

1 tax returns.

2
3 56. Form W-2 information frequently sells in the range of \$40 to \$50 per individual
4 between criminals on the internet.

5 57. Following a review by Mandiant, an outside security company that also
6 investigated the March 2017 TALX breach but somehow still failed to correct this vulnerability,
7 Equifax concluded that personal information relating to 143 million U.S. consumers – primarily
8 names, Social Security numbers, birth dates, addresses and, in some instances, driver's license
9 numbers were breached, in addition to credit card numbers for approximately
10 209,000 U.S. consumers, and certain dispute documents with credit and other personal identifying
11 information for approximately 182,000 U.S. consumers.
12

13
14 58. Since the breach, sources have reported that personal identifying information
15 accessed during the breach, including addresses, social security numbers, dates of birth and driver
16 license numbers for various celebrities and public figures are presently offered for sale on the
17 “Dark Web.”

18
19 59. The Dark Web is a portion of the internet that is not accessible with traditional web
20 browsers or through conventional search engines, but allows users with the proper system
21 configuration to anonymously browse hidden websites and communicate with each other via highly
22 encrypted messaging protocols.

23 60. While the Dark Web and its associated “TOR” browser technology is widely used
24 by criminals to traffic in various categories of illicit materials, including drugs, firearms,
25 professional hitman services, child pornography, and now apparently the private financial
26

1 information of most of the adult population of the United States of America previously maintained
2 by Equifax.

3
4 61. On September 20, 2017, Comodo Threat Intelligence Labs reported its findings that
5 the individuals that breached Equifax's system also injected malware into the system that was
6 successful in obtaining the login names and passwords of the highest executives at Equifax.

7
8 62. Using these credentials, the intruders were also able to exploit other services used
9 by Equifax, such as Dropbox and LinkedIn.

10 63. After obtaining the stolen credentials on the Dark Web and reviewing them,
11 Comodo found that Equifax's chief privacy officer, chief information officer, vice president of
12 public relations, and vice president of sales used passwords with major security deficiencies such
13 as all lowercase letters, no special symbols, and easily guessable words like spouses' names, city
14 names, and even combinations of initials and birth years.

15
16 **Equifax Refuses to Disclose the Fraudulent Procurement of Consumer Files**

17
18 64. Despite knowing about the breach in July, Equifax kept the information secret. It
19 did not reveal to individual consumers to whom it owed a contractual duty under a credit
20 monitoring service. And it did not reveal to the public—those whose information was stolen and
21 who stand to be injured from the breach—that the breach took place until September 8, 2017. But
22 even then, Equifax has not disclosed exactly who was affected and what information was accessed.
23 In the wake of the breach, Equifax's Chief Information Officer and Chief Security Officer have
24 "retired."
25

1 65. The credit report information fraudulently procured from Equifax is all that is
2 necessary to fraudulently obtain credit, tax returns and even a driver's license. With this
3 information, an identity thief can now open credit, obtain full credit files from other CRAs, and
4 even verify the falsified identity in future transactions.
5

6 66. Plaintiffs and class members will incur costs associated with time spent and the loss
7 of productivity from addressing and attempting to ameliorate, mitigate, and deal with the actual
8 and future consequences of the Data Breach, including finding fraudulent charges, cancelling and
9 reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of
10 withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance
11 of dealing with all issues resulting from the Data Breach; as well as damages to and diminution in
12 value of their personal and financial information entrusted to Equifax.
13
14

15 67. And Equifax knows this, as well as the urgency of providing detailed information
16 to victim consumers as soon as possible. It warns on its marketing site, "More than ever before,
17 your employees and customers are at great risk for identity theft and fraud. Over 165 million data
18 records of U.S. residents have been exposed due to data breaches since January 2005 - Privacy
19 Rights Clearinghouse."⁵
20

21 68. Defendants (now ironically) boast of how effective and robust its data breach
22 response time and program is, stating, "You'll feel safer with Equifax. We're the leading provider
23
24
25

26 5 <http://www.equifax.com/help/data-breach-solutions/> (last visited September 21, 2017).
27
28

1 of data breach services, serving more than 500 organizations with security breach events every
2 day. In addition to extensive experience, Equifax has the most comprehensive set of identity theft
3 products and customer service coverage in the market.” *Id.* Such “industry leading” services and
4 capabilities would, by Equifax’s suggestion require the breached business to, “Quickly inform
5 consumers[.]” *Id.*

6
7 69. Equifax has, however, not “quickly informed consumers” as to its own data breach.
8 As of the date of this filing, Equifax still refused to substantively inform affected consumers. And
9 Equifax waited at least six weeks before it publicly disclosed even the general fact of the data
10 breach.

11
12 70. Customers who called the dedicated call center set up by Equifax were often unable
13 to get a coherent or timely response.

14
15 71. Even the “free” credit monitoring it offered to hack victims came with a string. The
16 Terms of Service for TrustedID (an Equifax owned company) contain a provision that an
17 individual’s “membership subscription may be subject to automatic renewal.”⁶ Offering credit
18 monitoring to every American through TrustedID also positions Equifax to collect even more
19 valuable PII. To sign up, a consumer must authorize TrustedID to retrieve information about the
20 consumer from the other two credit bureaus (Equifax and TransUnion). The information on the
21 credit reports of the bureaus can vary by up to 20%, meaning Equifax can gain access to, and
22

23
24
25
26 6 <https://www.trustedid.com/serviceterms.php?serviceterms> (last visited Sept. 21, 2017).

1 ultimately profit from, additional information from the other two credit bureaus when consumers
2 grant TrustedID access to their Equifax and TransUnion credit files.

3
4 72. The system Defendants implemented to update consumers about whether their
5 credit reporting information had been procured by the identity thieves was ineffective and not
6 helpful. To take advantage of this look up, all you need to do is provide your last name and last
7 six (not 4) digits of your Social Security number. However, the website that Equifax launched
8 often returned the same message to a user regardless of what information was put in.⁷ And, the
9 site is not hosted on the Equifax network and appears to be a website domain and structure that
10 was previously recognized as critically vulnerable to a hack. Since trust is critical for web sites
11 like this, especially after a breach of this severity, it is difficult for consumers to trust that Equifax
12 latest online support option is properly protecting their data.
13

14
15 73. Regardless, even assuming the class members did not suffer a false positive,
16 Equifax has still refused to provide any detailed information as to what specific data was procured
17 for individual consumers. And the generalized summary of the fact that they produced data
18 including personal identifying information and some credit card account numbers is of little
19 comfort to Plaintiffs and class members. What specific documents or files were procured
20 containing such information? What additional parts of the credit report file was obtained? Which
21

22
23
24
25
26 ⁷ <https://www.riskbasedsecurity.com/2017/09/equifd-equifax-breach-response-off-to-a-rough-start/> (last visited September 21, 2017).

1 database(s) were hacked and thus procured? What information does Equifax have as to who
2 procured it?
3

4
5 **COUNT I: BREACH OF DUTY OF CARE**
6 ***Class Action Claim***

7 74. Plaintiffs restate each of the allegations in the preceding paragraphs as if set forth
8 at length herein.

9 75. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs brings this
10 action for themselves and on behalf of a class (the “National Breach Class”) defined as:

11 All natural persons residing in the United States (including all
12 territories and other political subdivision) whose consumer reporting information
13 at Equifax was procured as a result of the data breach announced by Equifax on or
14 about September 7, 2017.
15

16
17 The Class does not include Defendant’s officers, directors, and
18 employees; Defendant’s attorneys; Plaintiffs’ attorneys; any Judge overseeing or
19 considering this action together with members of their immediate family and any
20 judicial staff.
21

22
23 76. In addition, Plaintiffs allege a subclass limited to members of the National Breach
24 Class for whom Defendant’s records show that the primary address of that consumer as of May 1,
25 2017 was in Arizona.
26

1 77. The class and subclass, which each number above 100,000 consumers are so
2 numerous that joinder of all members is impractical.

3
4 78. There are questions of law and fact common to the class, which common issues
5 predominate over any issues involving only individual class members. For example, and without
6 limitation: (a.) whether Equifax had a duty of care to maintain the security of class member credit
7 reporting information; (b.) whether Equifax's duty was heightened; and (c.) whether Equifax
8 breached that duty in its failure to secure class member data.

9
10 79. Plaintiffs' claims are typical of those of the class members. All are based on the
11 same facts and legal theories. The tort alleged is the same and the class claim will rise and fall
12 entirely based upon whether or not Plaintiffs' claim rises or falls.

13
14 80. The Plaintiffs will fairly and adequately protect the interests of the class. The
15 Plaintiffs have retained counsel experienced in handling class actions and litigation against
16 Equifax as well as involving consumer credit reporting data and privacy protections. Neither
17 Plaintiffs nor their counsel have any interests that might cause them not to vigorously pursue this
18 action. The Plaintiffs are aware of their responsibilities to the putative classes and have accepted
19 such responsibilities.

20
21 81. Certification of a class under Rule 23(b)(1) of the Federal Rules of Civil Procedure
22 is proper. Prosecuting separate actions by or against individual class members would create a risk
23 of adjudications with respect to individual class members that, as a practical matter, would be
24 dispositive of the interests of the other members not parties to the individual adjudications or would
25 substantially impair or impede their ability to protect their interests.

1 82. Certification of a class under Rule 23(b)(2) of the Federal Rules of Civil Procedure
2
3 is appropriate in that Equifax has acted on grounds generally applicable to the class thereby making
4 appropriate declaratory relief with respect to the class as a whole.

5 83. Certification of the class under Rule 23(b)(3) of the Federal Rules of Civil
6 Procedure is also appropriate in that:

7 a. As alleged above, the questions of law or fact common to the members of the
8 classes predominate over any questions affecting an individual member. Each of the common
9 facts and legal questions in the case overwhelm the more modest individual damages issues.
10 Further, those individual issues that do exist can be effectively streamlined and resolved in a
11 manner that minimizes the individual complexities and differences in proof in the case.
12

13 b. A class action is superior to other available methods for the fair and efficient
14 adjudication of the controversy. Consumer claims generally are ideal for class treatment as they
15 involve many, if not most, consumers who are otherwise disempowered and unable to afford and
16 bring such claims individually. Further, most consumers affected by Equifax's tortious conduct
17 would likely be unaware of their rights under the law, or who they could find to represent them in
18 federal litigation. Additionally, individual litigation of the uniform issues in this case would be a
19 waste of judicial resources. The issues at the core of this case are class wide and should be resolved
20 at one time. One win for one consumer would set the law as for every similarly situated consumer.
21

22 84. Equifax knew or should have known the risks inherent to its possession of massive
23 amounts of sensitive personal information, including that (a) hackers would target Equifax, as a
24 dominant player in the consumer credit reporting and data aggregation industry, in order to acquire
25
26

1 such information; (b) the risk of sophisticated cyberattacks was continual and increasing; (c) its
2 own lax protocols had resulted in prior data breaches; (d) measures were available to adequately
3 address its cybersecurity deficiencies; and (e) failure to implement adequate cybersecurity
4 practices would result in a data breach.
5

6 85. Equifax's conduct in failing to protect Class Members' information, as described
7 above, constitutes negligence. Equifax had a duty to act as would a reasonable CRA to safeguard
8 the personal financial information of consumers entrusted to it by federal and state statutes.
9 Equifax breached that duty by failing to secure its systems, including but limited to, applying a
10 simple security patch that had been released for months prior to the break-in, then failing for
11 months to notify class members that their information was compromised. As a proximate result
12 of this breach of duty, National Breach Class Members suffered injuries. Those injuries resulted
13 in monetary damages to Plaintiffs and Class Members.
14
15

16 86. Equifax breached its duties to Plaintiffs and the Class through its conduct alleged
17 herein. Equifax had the ability to protect Class Members' PII from the cyberattack resulting in the
18 Data Breach, but failed to do so. Equifax failed to implement reasonable or adequate data security
19 practices to protect the type and scale of information in its possession, failed to timely detect the
20 cyberattack, utilized outdated and otherwise improper security measures and techniques, failed to
21 properly segment and patch systems containing sensitive consumer data, failed to disclose the
22 flaws in its data security, and failed to provide timely notice of the Data Breach.
23

24 87. Equifax would have been able to prevent and/or limit the harm caused by the Data
25 Breach had it maintained adequate protocols and security measures as alleged herein.
26
27
28

1 88. Defendants are also strictly liable for the data breach as Equifax owed a duty
2 because of the uniquely heightened and financially dangerous nature of its business and business
3 practices.
4

5 89. Plaintiffs and each class member has suffered actual harm and actual damages as a
6 result of this breach, for which Plaintiffs seek remedy and judgment.
7

8 **WHEREFORE**, Plaintiffs demand judgment and relief as pled and as
9 follows:

10 A. That an order be entered certifying the proposed Classes under Rule 23 of the
11 Federal Rules of Civil Procedure and appointing Plaintiffs and their counsel to represent them;

12 B. That judgment be entered against Defendants as pled for actual, statutory, treble
13 and punitive damages;
14

15 C. That the Court award costs and reasonable attorney's fees, pursuant to 15 U.S.C.
16 §§ 1681o and n;

17 D. That the Court grant disgorgement, rescission and other injunctive and declaratory
18 relief as pled, and requiring Equifax to make the full disclosures otherwise required to class
19 members;
20

21 E. That the Court grant such other and further relief as may be just and proper.

22 **PLAINTIFFS DEMAND TRIAL BY JURY**

23 **Respectfully,**

24 **CORINNE COOPER, MORGAN**
25 **RUTHERFORD, DONNA DECONCINI,**
26 *on behalf of themselves and all others*
27 *similarly situated,*
28

By: /s/ Susan M. Rotkis

Susan M. Rotkis, AZ Bar 032866
Consumer Litigation Associates West, PLLC
382 S. Convent Ave.
Tucson, AZ 85716
520-622-2481
srotkis@clalegal.com

Leonard A. Bennett
admission pro hac vice requested
Consumer Litigation Associates, P.C.
763 J. Clyde Morris Blvd, Suite 1-A
Newport News, VA 23601
757-930-3660
lenbennett@clalegal.com